https://doi.org/10.46991/S&L/2022.94.158

ԹՎԱՅԻՆ ԽՈՒԶԱՐԿՈՒԹՅՈՒՆԸ ՈՐՊԵՍ ՔՆՆՉԱԿԱՆ ՆՈՐ ԳՈՐԾՈՂՈՒԹՅՈՒՆ ՀՀ ՔՐԵԱԿԱՆ ԴԱՏԱՎԱՐՈՒԹՅԱՆ ՆՈՐ ՕՐԵՆՍԳՐՔԻ ՀԱՄԱՏԵՔՍՏՈՒՄ

Լառա Պետրոսյան
ԵՊՀ քրեական դատավարության և կրիմինալիստիկայի ամբիոնի հայցորդ,
ՀՀ Մարդու իրավունքների պաշտպանի օգնական

20-րդ դարի վերջերից տեղեկատվական-հաղորդակցական տեխնոլոգիաները դարձել են մարդկանց կյանքի անբաժանելի մասը, և դրանց դերը գնալով աճում է: Հասարակական կյանքի արմատական փոփոխությունները, որոնք տեղի են ունեցել թվայնացման, տեղեկատվական տեխնոլոգիաների՝ հասարակության կյանք ներդրման և համակարգչային ցանցերի շարունակվող գլոբալիզացիայի պատճառով, ստեղծել են հանցագործությունների կատարման նոր միջավայր: Կիբեռհանցագործությունները նոր մարտահրավեր են հասարակության համար, որոնց դեմ պայքարը յուրաքանչյուր իրավական պետության առաջնային նպատակներից պետք է լինի:

Համակարգչային համակարգերում պահվող թվային տվյալները կարող են կարևոր նշանակություն ունենալ քրեական գործի համար ոչ միայն կիբեռհանցագործությունների պարագայում, այլև ցանկացած հանցագործություն քննելիս: Ինչպես նշեցինք, տեղեկատվական տեխնոլոգիաների ներդրմամբ ձևավորված վիրտուալ իրականությունը դարձել է յուրաքանչյուրի կյանքի անբաժանելի մասը, և դրանք կարող են պարունակել ապացուցողական նշանակության տվյալներ:

Քրեադատավարական ապացուցման վերաբերյալ ծագող հարաբերությունները չեն կարող անմասն մնալ հասարակության վերոնշյալ զարգացումներից: Քրեական դատավարության օրենսգիրքը պետք է պատշաճ գործիքակազմով ապահովի իրավակիրառին՝ դրանք ապացուցողական զանգված ներառելու համար: Համապատասխան լիազորությունների բացակայությունը կարող է խոչընդոտել քննչական մարմիններին պատշաճ իրականացնել իրենց առջև դրված խնդիրները: Ելնելով քրեական գործերի լրիվ, օբյեկտիվ, բազմակողմանի քննություն իրականացնելու պահանջից՝ անհրաժեշտ է քրեադատավարական գործիքները հարմարեցնել էլեկտրոնային տեղեկատվական համակարգերի յուրահատկություններին[1]:

Կիբեռհանցագործությունների դեմ պայքարի և էլեկտրոնային ապացույցների ձեռքբերման վերաբերյալ հիմնական միջազգային իրավական փաստաթուղթը Եվրոպայի խորհրդի «Կիբեռհանցագործությունների մասին» կոնվենցիան է (այսուհետ՝ Բուդապեշտի կոնվենցիա), որը սահմանում է կիբեռհանցագործությունների դեմ պայքարի հիմնական սկզբունքները, այդ թվում՝ քրեադատավարական միջոցները:

Քրեական դատավարության նոր օրենսգրքում (ընդունված 05.05.2021 երկրորդ ընթերցմամբ և ամբողջությամբ, սակայն դեռևս գործողության մեջ չդրված) **(այսուհետ՝ Նոր օրենսգիրք)** քննչական գործողությունների թվում նախատեսվել է **թվային խուզարկությունը** որպես ինքնուրույն քննչական գործողություն: Այս ինստիտուտը նորություն է քրեադատավարական իրավունքում, և մինչ վերոնշյալ փոփոխությունները էլեկտրոնային տվյալների ձեռքբերումը իրականացվել է ավանդա-

---

[1] Տե՛ս Recommendation No R (95) 13 Of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers` Deputies):

կան զննման շրջանակներում:

Սույն աշխատանքում մեր առջև դրված խնդիրներն են *բացահայտել թվային խուզարկության՝ որպես ինքնուրույն քննչական գործողություն սահմանելու նպատակահարմարությունը, վերլուծել ՀՀ քրեական դատավարության նոր օրենսգրքում նախատեսված հայրենական իրավունքի համար նորություն հանդիսացող ինստիտուտը, ներկայացնել դրա առավելություններն ու թերությունները՝ միաժամանակ անդրադառնալով դրա համապատասխանությանը միջազգային չափանիշներին:*

Մինչ նշված հարցերին անդրադառնալը անհրաժեշտ է հստակեցնել, թե ինչ տեսակի էլեկտրոնային տեղեկատվություն է ակնկալվում ձեռք բերել թվային խուզարկության շրջանակում: Թեև ՀՀ օրենսդրությամբ ամրագրված չեն էլեկտրոնային տեղեկատվության հասկացությունը և դրա տեսակները, սակայն այսպիսի տարանջատում առկա է Բուդապեշտի կոնվենցիայում, Եվրոպայի խորհրդի, Կիբեռհանցագործությունների կոմիտեի զեկույցներում: Ընդ որում այս տարանջատումը էական նշանակություն ունի նաև գործնականում, մասնավորապես, քրեադատավարական միջոցառումների կիրառման առումով: Եվրոպայի խորդուրդն ամրագրել է, որ Բուդապեշտի կոնվենցիայում նախատեսված ընթացակարգերը ընդհանուր առմամբ ուղղված են բոլոր տեսակի համակարգչային տեղեկատվության ձեռքբերմանը, որոնք են՝ բաժանորդի վերաբերյալ տեղեկատվությունը (subscriber data), ընթացքի վերաբերյալ տեղեկատվություն (traffic data), բովանդակային տեղեկատվությունը (content data): Համակարգչային բոլոր տեսակի տվյալները կարող են գոյություն ունենալ երկու ձևով՝ պահված և հաղորդակցության ընթացքի մեջ (stored or in the process of communication): Ընդ որում յուրաքանչյուր քրեադատավարական գործողության կիրառելիությունը կապված է տեղեկատվության բնույթի և ձևի, ինչպես նաև գործողության բնույթի հետ[1]:

Նոր օրենսգրքի 236-րդ հոդվածի 1-ին մասի համաձայն՝ *թվային խուզարկությունը էլեկտրոնային սարքերում կամ կրիչներում պարունակվող թվային տվյալների որոնումն է:*

Թվային խուզարկության օրենսդրական բնորոշումից կարելի է ենթադրել, որ այս գործողությունն ուղղված է էլեկտրոնային կրիչներում պահված էլեկտրոնային տեղեկատվության ձեռքբերմանը, այսինքն՝ այս միջոցառումը չի կարող կիրառվել, երբ խոսքը հաղորդակցության ընթացքի մեջ գտնվող տեղեկատվության մասին է: Այդ դեպքում անհրաժեշտ է կատարել այլ գործողություններ: Բուդապեշտի կոնվենցիան պարունակում է դրույթներ այս տեսակ տեղեկատվության ձեռքբերման քրեադատավարական գործողության վերաբերյալ, մասնավորապես՝ այդպիսին են հանդիսանում պահված համակարգչային տվյալների որոնումը և առգրավումը (հոդված 19), ուստի թվային խուզարկության համապատասխանությունը միջազգային չափանիշներին դիտարկելու համար քննարկման առարկա ենք դարձրել հենց էլեկտրոնային սարքավորումներում պահված էլեկտրոնային տեղեկատվության որոնման և առգրավման ընթացակարգերը:

Եվրոպայի խորհուրդը, անդրադառնալով համակարգչային տեղեկատվության որոնմանը, արձանագրել է, որ այն արդյունավետ դարձնելու համար անհրաժեշտ է նախատեսել լրացուցիչ ընթացակարգային պահանջներ: Դրա համար առկա են մի քանի պատճառ, առաջինը՝ էլեկտրոնային տվյալները ոչ նյութական տեսք ունեն, երկրորդ՝ տեղեկատվությունը կարող է ընթերցվել համակարգչային սարքավորման միջոցով, սակայն այն չի կարող առգրավվել և այլ տեղ տարվել: Այս պարագայում տեղեկատվության առգրավումը պետք է իրականացվի դրա նյութական կրիչի առգրավմամբ կամ այդ տեղեկատվության պատճենահանմամբ՝ նյութական տեսք հա-

[1] Explanatory report to the Convention on Cybercrime, Council of Europe, European treaty series No 185 Budapest 23.11.2001, պարբերություն 136:

ղորդելով (օրինակ՝ print) կամ այլ կրիչի վրա ամրագրելով: Ներպետական օրենսդրությունը այսպիսի պատճենումներ կատարելու հնարավորություն պետք է նախատեսի: Երրորդ, համակարգչային համակարգերի փոխկապակցվածության պատճառով համակարգչային տեղեկատվությունը կարող է պահված չլինել որոնվող համակարգչում, սակայն հասանելի լինել այդ համակարգի համար: Որոնվող տեղեկատվությունը կարող է պահված լինել այլ կրիչի վրա, որը փոխկապակցված է սկզբնական համակարգչի հետ ուղղակիորեն կամ անուղղակիորեն հաղորդակցական համակարգերի միջոցով, օրինակ՝ համացանցի[1]:

Թվային խուզարկության՝ որպես ինքնուրույն քննչական գործողության սահմանման նպատակահարմարության վերաբերյալ եզրակացություններ կատարելու համար անհրաժեշտ է վերլուծել նաև գործող օրենսդրության կարգավորումները: Գործող քրեադատավարական օրենսգրքի (այսուհետ՝ **Օրենսգիրք**) կարգավորումների համատեքստում էլեկտրոնային տվյալների հետազոտումն իրականացվում է զննում քննչական գործողության շրջանակում:

Զննությունը վարույթն իրականացնող մարմնի կողմից տարբեր օբյեկտների անմիջական ուսումնասիրությունն է՝ հանցագործության հետ կապված տվյալներ ստանալու և քրեական գործով վարույթի ընթացքում դրանք օգտագործելու նպատակով[2]: **Օրենսգրքի 217-րդ հոդվածի համաձայն՝** *հանցագործության հետքերը, այլ նյութական օբյեկտները հայտնաբերելու, հանցագործության դեպքը, ինչպես նաև գործի համար նշանակություն ունեցող մյուս հանգամանքները պարզելու նպատակով քննիչը կատարում է տեղանքի, շինությունների, առարկաների, փաստաթղթերի, կենդանիների, մարդու կամ կենդանու դիակի զննում:*

Վերոնշյալ նորմի վերլուծությունը թույլ է տալիս եզրահանգել, որ օրենսդիրը տարբերակում է զննության հետևյալ տեսակները՝ տեղանքի, շինությունների, առարկաների, փաստաթղթերի, կենդանիների, մարդու կամ կենդանու դիակի զննություն, որոնք կարող են գործի համար նշանակություն ունեցող հանգամանքները պարզելու միջոց լինել: Քննարկենք փաստաթղթերի և առարկաների զննում իրականացնելու շրջանակներում էլեկտրոնային տվյալները հետազոտելու իրավաչափությունը:

Առարկաների զննության նպատակն է այն հատկանիշների պարզաբանումը, որոնք ընդգծում են տվյալ օբյեկտի և քրեական գործով ապացուցման ենթակա առարկաների միջև եղած կապը[3]: Միանշանակ է, որ էլեկտրոնային տեղեկատվության կրիչները, որում պարունակվում են թվային տվյալները, ի վերջո առարկաներ են: Սակայն ապացուցողական նշանակություն ունի ոչ թե տեղեկատվության կրիչը իր արտաքին հատկանիշներով, այլ դրա բովանդակությունը, դրանում ամրագրված տվյալները: Այս համատեքստում պետք է արձանագրել, որ թեև էլեկտրոնային տեղեկատվությունն ամրագրված է նյութական կրիչի վրա, սակայն ունի թվային տեսք և հանդիսանում է վիրտուալ աշխարհի օբյեկտ և չունի նյութական արտահայտություն:

Խոսելով էլեկտրոնային տեղեկատվության կրիչներից՝ ուշադրության են արժանի տեղեկատվության օնլայն կրիչները, որոնք տարբեր կազմակերպությունների կողմից մատուցվող օնլայն ծառայությունների տարատեսակ են (iCloud, Облако Mail.Ru, Dropbox, Google Drive, Яндекс.Диск և այլն): Այս տեսակի կրիչները տեսանելի չեն և հանդիսանում են օնլայն սերվերներ: Թեև թվային տեղեկատվությունն արձանագրված է նյութապես գոյություն ունեցող սերվերների վրա, սակայն դրանք ֆիզիկապես կարող են գտնվել աշխարհի ցանկացած անկյունում: Այսպես, ելնելով

---

[1] Explanatory report to the Convention on Cybercrime, Council of Europe, European treaty series No 185 Budapest 23.11.2001, պարբերություն 187

[2] Տե՛ս **Ենգիբարյան Վ.Գ.** Առանձին քննչական գործողությունների կատարման տակտիկա, Գիտ. ձեռ., Երևան, 2018, էջ 175:

[3] Տե՛ս նույն տեղը, էջ 233:

էլեկտրոնային տեղեկատվության կրիչների առանձնահատկություններից՝ դրանք երբեմն անհնար է ձեռք բերել և կցել գործի նյութերին: Այս պայմաններում էլ ավելի է կարևորվում գործի համար նշանակություն ունեցող տվյալներ պարունակող տեղեկատվությունը նյութական կրիչից զատ որպես ապացույց դիտարկելը:

Բացի այդ՝ էլեկտրոնային տեղեկությանը բնութագրական չէ կրիչի հետ կապի սերտությունը: Էլեկտրոնային տեղեկատվությունը կարող է տեղափոխվել տարբեր կրիչների վրա, պատճենահանվել և այլն: Այս տեսանկյունից էլկետրոնային տեղեկատվությունը որպես ապացույց դրա կրիչից զատ դիտարկելը ևս էական է:

Գործող օրենսդրության կարգավորումների համատեքստում առավել նպատակահարմար է էլեկտրոնային տեղեկատվության զննման իրականացումը փաստաթղթերի զննում գործողության շրջանակներում: Փաստաթուղթ հասկացության լայն մեկնաբանումը հնարավորություն է տալիս այս գործողության շրջանակում իրականացնել էլեկտրոնային տեղեկատվության ուսումնասիրություն:

Սակայն այս առումով հարկ է նկատել, որ **«էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին» օրենքի** 2-րդ հոդվածի համաձայն՝ *էլեկտրոնային փաստաթուղթը՝ տեղեկություն գրանցված նյութական կրիչի վրա էլեկտրոնային եղանակով, վավերացված էլեկտրոնային թվային ստորագրությամբ*: Այս հասկացությունը չի ընդգրկում ողջ էլեկտրոնային տեղեկատվությունը, էլեկտրոնային փաստաթուղթը հարաբերակցվում է թվային տեղեկատվության հետ, ինչպես մասն ամբողջի հետ: Այսպես, ամեն էլեկտրոնային փաստաթուղթ թվային տեղեկատվության տեսակ է, բայց թվային տեղեկատվությունը միշտ չէ, որ էլեկտրոնային փաստաթուղթ է: Վերջինիս տարբերակման չափանիշ է էլեկտրոնային թվային ստորագրության առկայությունը:

Այսպիսով, ի տարբերության գործող օրենսդրության կարգավորումների, Նոր օրենսգրքում ամրագրված թվային խուզարկության ձևակերպումը հնարավորություն է տալիս էլեկտրոնային կրիչները դիտարկել թվային տվյալներից առանձնացված: Այս տարանջատումը կարևոր նշանակություն ունի էլեկտրոնային տեղեկատվության և դրա կրիչների առանձնահատկությունների համատեքստում: Ինչպես արդեն նշել ենք, ապացուցողական նշանակություն ունի ոչ թե տեղեկատվության էլեկտրոնային կրիչը իր ֆիզիկական արտաքին հատկանիշներով, այլ դրանում ամրագրված էլեկտրոնային տեղեկատվությունը, իսկ էլեկտրոնային տվյալները չեն կարող լինել առարկայական: Խնդիրն ավելի է խորանում համացանցում տեղադրված տեղեկատվությունը հետազոտելու դեպքում, այս պարագայում էլեկտրոնային տվյալների կրիչ է վիրտուալ տարածությունը, որը չունի առարկայական արտահայտություն:

Դրական փոփոխություն է նաև պատճենահանման հնարավորության նախատեսումը թվային խուզարկության շրջանակում: Հարկ է նկատել, որ գործող օրենսդրությամբ այսպիսի հնարավորություն նախատեսված չէ:

Անդրադառնալով էլեկտրոնային ապացույցների ձեռքբերման եղանակներին՝ Եվրոպայի խորհուրդն արձանագրել է, որ դրանք կարող են ձեռք բերվել հետևյալ ճանապարհներով.

1. Նյութական կրիչների առգրավում, որոնց վրա պահվում է ոչ նյութական տեղեկատվությունը,

2. էլեկտրոնային տեղեկատվության պատճենահանում և ամրագրում թղթային տարբերակում,

3. էլեկտրոնային տեղեկատվության պատճենահանում և ամրագրում այլ նյութական կրիչի վրա[1]*:*

Գործող քրեադատավարական օրենսդրության վերլուծությամբ հանգում ենք

[1] Explanatory report to the Convention on Cybercrime, Council of Europe, European treaty series No 185 Budapest 23.11.2001, պարբերություն 185:

այն հետևության, որ այն էլեկտրոնային ապացույցների Եվրոպայի խորհրդի սահմանած եղանակներից նախատեսում է միայն էլեկտրոնային տեղեկատվության կրիչների առգրավման եղանակը: Ինչ վերաբերում է էլեկտրոնային պատճենահանմանը, ապա այն ընդգրկված չէ քննչական կամ դատավարական գործողությունների շարքում, ինչպես նաև չի հանդիսանում որևէ այլ քննչական գործողության մաս:

Նոր օրենսգիրքը նախատեսել է նաև պատճենահանման եղանակով թվային տվյալները վերցնելու հնարավորությունը: Այսպես՝

Նոր օրենսգրքի 236-րդ հոդվածի 2-րդ մասի համաձայն՝ *վարույթի համար նշանակություն ունեցող տվյալները վերցվում են այլ կրիչի վրա պատճենելու եղանակով՝ ապահովելով այդ տվյալների և դրանցից կատարված պատճենների ամբողջականությունը:*

Նոր օրենսգրքի 239-րդ հոդվածի 1-ին համաձայն՝ *առգրավումը վարույթի համար նշանակություն ունեցող և ստույգ հայտնի տեղում կամ անձի մոտ գտնվող որոշակի առարկաներ, նյութեր, թվային տվյալներ կամ փաստաթղթեր քննիչի նախաձեռնությամբ վերցնելն է:* **Նույն հոդվածի 10-րդ մասի համաձայն՝** *էլեկտրոնային սարքերում կամ կրիչներում պարունակվող թվային տվյալներն առգրավվում են այլ կրիչի վրա պատճենելու եղանակով՝ ապահովելով այդ տվյալների և դրանցից կատարված պատճենների ամբողջականությունը:*

Վերլուծելով սույն դրույթները՝ կարելի է եզրակացնել, որ էլեկտրոնային սարքերի և կրիչների բովանդակության խուզարկության արդյունքում հայտնաբերված վարույթի համար նշանակություն ունեցող, թվային տեսք ունեցող տվյալները վերցվում են պատճենահանման միջոցով:

Էլեկտրոնային պատճենահանումը հնարավորություն կտա վարույթն իրականացնող մարմիններին վերցնել անհրաժեշտ տեղեկատվությունը՝ միաժամանակ երկարաժամկետ չզրկելով դրա կրիչի տիրոջը իր սեփականության իրավունքից: Հաճախ ապացուցողական նշանակություն ունեցող տեղեկությունից բացի, առգրավվող էլեկտրոնային կրիչների վրա լինում են դրանց սեփականատերի համար կարևոր տվյալներ, որոնք կապ չունեն քրեական գործի հետ: Այդպիսի տեղեկատվությունը սեփականատերի կողմից օգտագործելու անհնարինությունը կարող է վերջինիս պատճառել անարդարացի վնաս:

Միաժամանակ պատճենահանման հնարավորության նախատեսումը չպետք է մեկնաբանվի այնպես, որ էլեկտրոնային կրիչների առգրավումը բացառվի: Որոշ դեպքերում էլեկտրոնային կրիչների առգրավումը էլեկտրոնային ապացույցների ձեռքբերման անփոխարինելի միջոց է: Հարկ է նկատել, որ Բուդապեշտի կոնվենցիայում «առգրավում» եզրույթը ներառում է նյութական կրիչի առգրավումը և համակարգչային տվյալների պատճենահանումը, որոնք պետք է կիրառվեն ըստ գործի հանգամանքների:

Համակարգչային տեխնիկայի միջոցների առգրավումն ունի մի շարք առավելություններ: Այն արագացնում է քննության ընթացքը և չի պահանջում բարձր որակավորում ունեցող մասնագետի ներկայություն: Բացի այդ՝ այն հնարավորություն է տալիս ավելի մանրամասն ուսումնասիրել դրանում ամրագրված տեղեկատվությունը և բացառում է հետաքրքրություն ներկայացնող տվյալները բաց թողնելու ցանկացած հնարավորություն[1]:

Եվրոպայի խորհուրդն արձանագրել է, որ մի շարք դեպքերում, երբ տեղեկատվությունը պահված է յուրահատուկ հաղորդակցական համակարգերում, և հնարավոր չէ տվյալների պատճենահանում, անխուսափելի է կրիչի առգրավումը: Առգրա-

[1] Տե՛ս **Зуев С.В., Осовянников Д.В.** Копирование электронной информации в теории и практике уголовного процесса 2014, էջ 170 https://cyberleninka.ru/article/n/kopirovanie-elektronnoy-informatsii-v-teorii-i-praktike-ugolovnogo-protsessa

վումը կարող է անհրաժեշտ լինել նաև այն դեպքերում, երբ տեղեկատվության կրիչը պետք է փորձաքննվի և հետազոտվի՝ վերականգնելու համար այն տվյալները, որոնք ոչնչացվել կամ փոփոխվել են, սակայն թողել են որոշակի հետքեր[1]: Տեղեկատվության պատճենահանումը չպետք է թույլատրվի նաև այն դեպքերում, երբ այն կարող է խոչընդոտել հանցագործության քննությունը, կամ էլ կարող է վնասել կամ ոչնչացնել ինֆորմացիան[2]:

Դատավարագետ Օ.Վ. Օվչիննիկովան նշում է, որ, կախված տեղեկատվության նյութական կրիչից, անհրաժեշտ է տարբերակել թվայնացված տեղեկություններ հավաքելու ճանապարհները[3]: Կհամաձայնենք դատավարագետի այն տեսակետի հետ, որ անհրաժեշտ է հաշվի առնել էլեկտրոնային տեղեկատվության կրիչների որոշ հատկանիշներ, քանի որ այն չի կարող գոյություն ունենալ նյութական կրիչից դուրս:

Այսպես, էլեկտրոնային տեղեկատվության կրիչները լինում են էներգիայից կախված և անկախ: **էներգիայից կախված կրիչների** առանձնահատկությունն այն է, որ սնուցումը անջատելու դեպքում կրիչների վրայի տեղեկատվությունը կարող է վերանալ (օրինակ՝ օպերատիվ հիշողություն ունեցող սարքավորումները): Այդ սարքավորումների հետազոտումը հնարավոր է միայն միացված լինելու դեպքում, այսինքն՝ դեպքի վայրում խուզարկություն կատարելու միջոցով: Այլ եղանակով, օրինակ՝ տեխնիկահամակարգչային փորձաքննության միջոցով, այդպիսի կրիչի վրա առկա տեղեկատվությունը զննելու հնարավորություն չկա[4]: Այսպիսով, այս դեպքում անհրաժեշտ է կատարել խուզարկություն հենց դեպքի վայրում, իսկ հայտնաբերված տեղեկատվության կորուստ թույլ չտալու համար պատճենահանել տեղեկատվությունը և ամրագրել այլ նյութական կրիչի վրա:

էներգիայից անկախ կրիչների հետազոտումը, Ե.Ռ. Ռոսինսկայայի կարծիքով, առավել նպատակահարմար է իրականացնել տեխնիկահամակարգչային փորձաքննության միջոցով[5]: էներգիայից անկախ կրիչներն են, օրինակ՝ կոշտ, լազերային սկավառակները, USB ֆլեշ կրիչները և այլն: էլեկտրոնային կրիչների ամբողջական հետազոտումը կապված է դրանում պահվող հարյուրավոր փաստաթղթերի, համակարգչային ծրագրերի հետ, որոնց ուսումնասիրությունը երբեմն պահանջում է հատուկ սարքավորումներով հագեցած աշխատանքային միջավայր, հետազոտական հատուկ գիտելիքներ, համակարգչային ոլորտին տիրապետող փորձագետի մասնակցություն: Ելնելով վերոգրյալից՝ էներգիայից անկախ կրիչներից էլեկտրոնային տվյալներ ձեռքբերելու համար առավել արդյունավետ է կրիչի առգրավումը: Դրան կարող են հաջորդել փորձաննության իրականացումը կամ դրա պարունակության խուզարկությունը և հայտնաբերված տվյալների պատճենահանումը: Հաշվի առնելով պատճենահանում իրականացնելու հնարավորությունը՝ համաչափ չի լինի կրիչի սեփականատիրոջը երկար ժամանակով զրկել իր սեփականությունից:

Ամփոփելով վերոգրյալը՝ կարող ենք եզրահանգել, որ էլեկտրոնային տեղեկատվության պատճենահանում իրականացնելու լիազորություն իրավասու մարմնին վերապահելը ոչ միայն միջազգային պարտավորություն է, այլև պայմանավոր-

---

[1] Explanatory report to the Convention on Cybercrime, Council of Europe, European treaty series No 185 Budapest 23.11.2001, պարբերություն 196:

[2] Տե՛ս **Гаврилин Ю.В.** Электронные носители информации в уголовном судопроизводстве «Право», 2017, էջ 150:

[3] Տե՛ս **Овчиникова О.В.** Собирание электронных доказательств, размещенных в сети Интернет // Правопорядок: история, теория, практика. 2016, էջ 52:

[4] Տե՛ս **Зигура Н.А.** Компьютерная информация как вид доказательств в уголовном процессе России: дис. на соискание научной академической степени канд.юрид.наук. Челябинск, 2010, էջ 75

[5] Տե՛ս **Россинская Е.Р.** Судебная компютерно-техническая экспертиза. М., 2001, էջ 113:

ված է տարատեսակ թվային տվյալների առանձահատկություններով: Էլեկտրոնային պատճենահանումը հաճախ տվյալների ձեռքբերման ամենաանպատակահարմար, երբեմն միակ հնարավոր գործողությունն է, բացի այդ՝ կրկնօրինակում իրականացնելու հնարավորությունը բխում է վարույթի մասնավոր մասնակիցների շահերի ապահովման անհրաժեշտությունից:

Սակայն վերոնշյալը չի նշանակում, որ բոլոր դեպքերում հնարավոր է և նպատակահարմար է իրականացնել էլեկտրոնային պատճենահանում: Կրիչների առգրավումը որոշ դեպքերում մնում է անփոխարինելի գործողություն, մասնավորապես, այնպիսի իրավիճակներում, երբ անհնար է իրականացնել պատճենահանում, կամ վերջինս կարող է հանգեցնել տվյալների ոչնչացման կամ վնասման, ինչպես նաև այն դեպքերում, երբ անհրաժեշտ է իրականացնել փորձաքննություն տվյալները վերականգնելու կամ դրանց իսկությունը պարզելու նպատակով: Այսպես, էլեկտրոնային պատճենահանումը և էլեկտրոնային տեղեկատվության նյութական կրիչի առգրավումը ինքնուրույն ճանաչողական միջոցներ են, որոնք որոշակի պայմանների դեպքում կարող են փոխարինել կամ հաջորդել միմյանց: Խնդիրը տարբերակված մոտեցում ցուցաբերելու հնարավորության ապահովումն է, որն անհրաժեշտ է սահմանել քրեադատավարական օրենսդրությամբ: Արդյունավետությունը, նպատակահարմարությունը և մասնակիցներին պատճառվող հնարավոր վնասի նվազագույնի հասցնելը պետք է լինեն այն չափանիշները, որոնցով պետք է առաջնորդվեն վարույթն իրականացնող մարմինները:

Նոր օրենսգրքով փոփոխություններ են կատարվել նաև երաշխիքների առումով: Թվային խուզարկությունը, ի տարբերություն գործող կարգավորումների, դարձել է նախնական դատական վերահսկողության առարկա: **Նոր օրենսգրքի 209-րդ հոդվածի 4-րդ և 6-րդ մասերի համաձայն**՝ *բացառապես դատարանի որոշման հիման վրա են կատարվում թվային խուզարկությունը, էլեկտրոնային սարքերում կամ կրիչներում պարունակվող թվային տվյալների առգրավումը:*

Եվրոպայի խորհուրդը, անդրադառնալով էլեկտրոնային ապացույցների ձեռքբերման ընթացքում անհրաժեշտ պայմաններին և երաշխիքներին, կողմերի համար սահմանում է պարտավորություններ՝ ապահովելու մարդու իրավունքների և ազատությունների համապատասխան պաշտպանությունը. ներառյալ այն իրավունքները, որոնք բխում են Եվրոպայի խորհրդի Մարդու իրավունքների և հիմնարար ազատությունների 1950 թ. կոնվենցիայով (այսուհետ՝ ՄԻԵԿ), 1966 թ. ՄԱԿ-ի՝ Քաղաքացիական և քաղաքական իրավունքների միջազգային Դաշնագրով և մարդու իրավունքների մյուս կիրառելի միջազգային փաստաթղթերով ստանձնած պարտավորություններից: Հաջորդ երաշխիքը, որի մասին խոսվում է Կոնվենցիայում, համաչափության սկզբունքն է, որի համաձայն՝ բոլոր ընթացակարգերը պետք է համաչափ լինեն կատարված իրավախախտմանը:

Միևնույն ժամանակ Կոնվենցիայի 15-րդ հոդվածի 2-րդ մասի համաձայն՝ այսպիսի պայմանները և երաշխիքները պետք է, ելնելով առնչվող իրավասության և ընթացակարգի բնույթից, ի թիվս այլոց, ներառեն դատական կամ մյուս անկախ վերահսկողությունները: Հարկ է նկատել, որ էլեկտրոնային տեղեկատվության կրիչների բովանդակության զննումը առնչվում է ՄԻԵԿ 8-րդ հոդվածով նախատեսված մարդու անձնական և ընտանեկան կյանքը հարգելու իրավունքին:

Էլեկտրոնային կրիչների, հատկապես անհատական թվային սարքավորումների բովանդակությունն ուսումնասիրելիս մեծ է ռիսկը, որ վարույթն իրականացնող մարմինը բախվի անձնական տվյալներ պարունակող տեղեկատվությանը, ինչի արդյունքում կսահմանափակվի անձի անձնական կամ ընտանեկան կյանքը հարգելու իրավունքը: Ուստի հաշվի առնելով ՀՀ Սահմանադրությամբ, ինչպես նաև միջազգային մի շարք փաստաթղթերում ամրագրված իրավունքի սահմանափակման հնարավորությունը, անհրաժեշտ են լրացուցիչ դատական երաշխիքներ: Այսպես, վարույթն իրականացնող մարմինը պարտավոր է համապատասխան գործողութ-

յունները կատարելու թույլտվություն տալու խնդրանքով միջնորդություն ներկայացնել դատարան՝ հիմնավորելով իրավունքի այդ տեսակ սահմանափակման անհրաժեշտությունն ու իրավաչափությունը:

Մարդու իրավունքների եվրոպական դատարանը, անդրադառնալով ՄԻԵԿ 8-րդ հոդվածով նախատեսված իրավունքի սահմանափակմանը, արձանագրել է, որ դատարանի թույլտվության բացակայության դեպքում օրենքով սահմանված պայմաններն ու սահմանափակումները չափազանց թույլ են և լի բացթողումներով անձի իրավունքներին միջամտությունը լեգիտիմ նպատակին համաչափ դիտելու համար[1]:

Ուսումնասիրված միջազգային փորձը նույնպես վկայում է այն մասին, որ թվային կրիչների բովանդակության խուզարկությունը անհրաժեշտ է դարձնել նախնական դատական վերահսկողության առարկա: Այդպիսի երկրներ են օրինակ՝ Վրաստանը[2], Մոլդովան[3], Բոսնիա և Հերցեգովինան[4], Խորվաթիան[5], Ռումինիան[6], Բուլղարիան[7]:

Ամփոփելով վերոգրյալը՝ կարելի է եզրակացնել, որ էլեկտրոնային կրիչներում պարունակվող թվային տվյալների որոնումը պետք է իրականացվի միայն դատարանից ստացված թույլտվության դեպքում: Հետևաբար՝ Նոր օրենսգրքով թվային խուզարկությունը նախնական դատական վերահսկողության առարկա դարձնելը բխում է մարդու անձնական և ընտանեկան կյանքը հարգելու իրավունքից:

Անդրադառնալով համակարգչում պահված տվյալների որոնմանը՝ Եվրոպայի խորհուրդն արձանագրել է, որ համակարգչային համակարգերի փոխկապակցվածության պատճառով տեղեկատվությունը կարող է պահված չլինել խուզարկվող համարգչում, սակայն այն կարող է հասանելի լինել այդ համակարգի համար: Այն կարող է պահված լինել համագարչի հետ փոխկապակցված հիշողության սարքավորման կամ այնպիսի համակարգի մեջ, որը փոխկապակցված է անուղղակիորեն՝ հաղորդակցության համակարգերի միջոցով, օրինակ՝ համացանցի: Խուզարկությու-

[1] Տե՛ս Funke and Crémieux v. France and Miailhe v. France (no. 1), judgments of 25 February 1993, Series A nos. 256-B and 256-C

[2] https://www.coe.int/en/web/octopus/-/georgia?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2, հոդված 119

[3] https://www.coe.int/en/web/octopus/-/moldova-republic-of-?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

[4] https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/AZnxfNT8Y3Zl/content/bosnia-and-herzegovina?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_AZnxfNT8Y3Zl%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_pos%3D1%26p_p_col_count%3D2?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

[5] https://www.legislationline.org/download/id/7895/file/Croatia_Criminal_proc_code_am2009_en.pdf հոդված 242

[6] https://www.legislationline.org/download/id/5896/file/Romania_CPC_am2014_EN.pdf, հոդված 168

[7] https://sherloc.unodc.org/cld/uploads/res/document/bgr/1968/criminal_procedure_code_of_the_republic_of_bulgaria_html/Bulgaria_Criminal_Procedure_Code_2011.pdf

նը պետք է տարածվի այն կրիչների վրա, որոնցում տվյալներն իսկապես պահպանված են[1]:

Բուդապեշտի կոնվենցիայի 19-րդ հոդվածի 2-րդ կետը հնարավորություն է տալիս քննչական մարմիններին տարածելու որոնումը այլ համակարգչային համակարգի կամ դրա մի մասի վրա, այն դեպքում, երբ իրենք ունեն հիմքեր ենթադրելու, որ անհրաժեշտ տեղեկատվությունը պահվում է այդտեղ:

Այսպիսով, Բուդապեշտի կոնվենցիայի պահանջներից է նախատեսել այնպիսի օրենսդրական միջոցներ, որոնք հնարավորություն կտան համակարգչային համակարգում էլեկտրոնային տվյալների որոնման շրջանակում իրականացնել դրա հետ փոխկապակցված համակարգչային համակարգերի, սարքավորումների բովանդակության ուսումնասիրում, այն դեպքում, երբ այդ համակարգերը օրինական հասանելի են սկզբնական որոնվող համակարգի համար, և իրավասու մարմինները ողջամտորեն կարող են ենթադրել, որ փնտրվող տվյալները պահվում են մեկ այլ սարքավորման կամ համակարգի մեջ:

Այսպիսի կարգավորում նախատեսված է, օրինակ, Ռումինիայի քրեական դատավարության օրենսգրքում, որի 168-րդ հոդվածի համաձայն՝ այն դեպքում, երբ համակարգչային համակարգի կամ համակարգչային տեղեկատվության կրիչի բովանդակության որոնման ժամանակ հայտնաբերվում է, որ փնտրվող տվյալները պահված են այլ համակարգչային համակարգում, որը հասանելի է սկզբնական համակարգի համար, դատախազը կամ քննչական մարմինը պետք է անմիջապես հրամայի պահպանել և պատճենահանել համակարգչային տեղեկատվությունը և անհապաղ դիմի դատարան:

Խորվաթիայի քրեական դատավարության օրենսգրքի 257-րդ հոդվածի համաձայն՝ շարժական գույքի որոնումը ներառում է նաև համակարգիչների և սարքավորումների որոնումը, որը փոխկապակցված է համակարգչի կամ տեղեկատվությունը հավաքելու, պահպանելու, տեղափոխելու համար նախատեսված սարքավորման, հեռախոսի, տեղեկատվության կրիչների և այլ հաղորդակցությունների հետ:

Հաշվի առնելով վերոգրյալը՝ առաջարկում ենք նախատեսել Նոր օրենսգրքի 236-րդ հոդվածում հասանելի համակարգչային համակարգում էլեկտրոնային տվյալների որոնման հնարավորությունը հետևյալ խմբագրությամբ. «էլեկտրոնային սարքերի կամ կրիչների բովանդակությունը խուզարկելիս, երբ վարույթն իրականացնող մարմինը ողջամտորեն կարող է ենթադրել, որ որոնվող թվային տվյալները կարող են գտնվել էլեկտրոնային սարքի կամ կրիչի համար օրինականորեն հասանելի փոխկապակցված էլեկտրոնային սարքում կամ կրիչում, նա կարող է իրականացնել նաև այդ սարքավորման պարունակության խուզարկություն»:

Էլեկտրոնային տեղեկատվության առանձնահատկություններով պայմանավորված՝ ուշադրության է արժանի բազմաթիվ դատավարագետների կողմից քննարկման առարկա դարձած էլեկտրոնային կրիչների առգրավման և տեղեկատվության պատճենահանման ժամանակ մասնագետի պարտադիր մասնակցության հարցը: Հատկանշական է, որ ՌԴ օրենսդիրը սահմանել է, որ էլեկտրոնային տեղեկատվության կրիչները առգրավվում են **մասնագետի** պարտադիր մասնակցությամբ (ՌԴ ՔԴՕ 164.1 հոդվածի 2-րդ մաս)[2]:

Անդրադառնալով էլեկտրոնային տեղեկատվության կրիչների առգրավման և տեղեկատվության պատճենահանման ժամանակ մասնագետի մասնակցությանը՝ Ռ.Ա. Բելկինը նշում է, որ ՌԴ օրենսդիրը իրավացիորեն հաշվի է առել այն հանգամանքը, որ էլեկտրոնային տեղեկատվության կրիչների առգրավումը կարող է լինել

[1] Explanatory report to the Convention on Cybercrime, Council of Europe, European treaty series No 185 Budapest 23.11.2001, պարբերություն 187

[2] "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 02.08.2019), հասանելի է http://www.consultant.ru/document/cons_doc_LAW_34481/

բարդ առաջադրանք, որը պահանջում է ինֆորմատիկայի ոլորտի մասնագիտական գիտելիքներ[1]:

Ն.Ա. Իվանովը իրավացիորեն նշում է, որ տեխնիկահամակարգչային փորձաքննություն իրականացնող փորձագետների ներգրավումը որպես մասնագետ այն մեքենայական կրիչների վրա ամրագրված տեղեկատվության հայտնաբերման և վերցման համար, որոնք չեն կարող ֆիզիկապես տեղափոխվել դատափորձաքննական հաստատություն, կարևոր նշանակություն ունի: Այդպիսին կարող է լինել էներգիայի սնուցում պահանջող սարքավորման հետազոտությունը, մասնավորապես, իրականացվող ծրագրերի և գործընթացների վերլուծությունը, էներգիայից կախում չունեցող կրիչի վրա տեղեկատվության ամրագրումը[2]:

Այսպիսի իրավիճակ հնարավոր է նաև քննչական գործողությունների իրականացման ժամանակ միացված համակարգչի դեպքում: Վ.Ն. Կարագոդինը այս կապակցությամբ գրում է, որ համակարգի փոփոխական տվյալները անհայտանում են համակարգի անջատման դեպքում մինչև պատճենահանում և տեխնիկահամակարգչային փորձաքննություն իրականացնելը[3]: Նույնանման է նաև հայրենական դատավարագետ և կրիմինալիստ Վ.Գ Ենգիբարյանի մոտեցումը, ով նշում է հետևյալը. «Քննիչի համար դժվարություն հարուցող գործողություններից է համակարգչի անթույլատրելի մուտքի պաշտպանության հաղթահարումը: Սխալ մոտեցման դեպքում հնարավոր է պաշտպանված տվյալների ինքնաոչնչացում, փոփոխություն և քողարկում հատուկ ծրագրերի օգնությամբ: Համակարգիչների միացումը և անջատումը, դրանց միջոցով որևէ գործողության իրականացումը նպատակահարմար է իրականացնել տվյալ քննչական գործողության կատարմանը մասնակցող մասնագետի կողմից»[4]:

Միևնույն ժամանակ ուշադրության է արժանի նաև այն դատավարագետների կարծիքները, ըստ որոնց՝ մասնագետի մասնակցության պարտադիրությունը անպատակահարմար է: Այսպես, ըստ Օ.Վ.Օվչինիկովայի հետազոտության՝ ՌԴ-ում հարցված քննիչների 95%-ը նշում է, որ մասնագետի մասնակցությունը էլեկտրոնային տեղեկատվության կրիչների վերցնելուն խախտում է դատավարական տնտեսման սկզբունքը, հարցվածների 5%-ը համաձայնել է մասնագետի մասնակցության նպատակահարմարությանը այն դեպքերում, երբ առկա է անհրաժեշտություն կրիչները կապից անջատելու կամ սարքավորման ապամոնտաժմամբ դրա բաղկացուցիչ մասերը վերցնելու համար[5]: Ս.Վ. Զունը նշում է, որ էլեկտրոնային տեղեկատվության կրիչները կարող են առգրավվել առանց մասնագետի մասնակցության, եթե դրանք առգրավվում են ամբողջությամբ՝ առանց դրա բովանդակության պատճենահանման, և չի պահանջվում հատուկ գիտելիքներ: Նրա կարծիքով՝ քննիչին պետք է տրվի հնարավորություն ներգրավել մասնագետին տեղեկատվության էլեկտրոնային կրիչները վերցնելու դեպքում, երբ իսկապես անհրաժեշտ են հատուկ գիտելիքներ, իսկ ՔԴՕ իմպերատիվ պահանջը պարտադիր մասնակցության մասին չի համապատասխանում ժամանակի զարգացումներին[6]:

Ամփոփելով վերոշարադրյալ մոտեցումները՝ կարելի է կատարել հետևյալ եզրահանգումները: էլեկտրոնային տեղեկատվության ուսումնասիրության, պատճենահանման, էլեկտրոնային տեղեկատվության կրիչների առգրավման ժամանակ

---

[1]Տե՛ս **Белкин А.Р.** Теория доказывания в уголовном судопроизводстве Москва 2017, էջ 162:
[2]Տե՛ս **Зигура Н.А.** նշված աշխատության էջ 109:
[3] Տե՛ս **Карогодин В.Н. Кастомаорв К.В.** Некоторые проблемы судебной компьятерно-технический экспертизы. Челябинск 2009, էջ 311:
[4]Տե՛ս **Ենգիբարյան Վ.Գ.,** Հանցագործությունների քննության մեթոդիկա: ԵՊՀ հրատ. 2014, էջ 282:
[5]Տե՛ս **Овчиникова О.В.** նշված աշխատության էջ 153:
[6]Տե՛ս Зуев С.В. նշված աշխատության էջ 195:

մասնագետի մասնակցությունը որոշ դեպքերում անհրաժեշտ է: Մասնավորապես, երբ խոսքը էներգիայից կախում ունեցող սարքավորումների մասին է, համակարգչային հանցագործությունների դեպքի վայրի զննության և այլ քննչական գործողությունների ժամանակ մասնագետի մասնակցությունը պարտադիր է: Տեխնիկական սխալները կարող են հանգեցնել ապացուցողական նշանակություն ունեցող տեղեկավության կորստի, իսկ վարույթն իրականացնող մարմինները երբեմն չեն տիրապետում այդպիսի հատուկ գիտելիքների: Միևնույն ժամանակ մասնագետի պարտադիր մասնակցության իմպերատիվ պահանջը թերևս ծայրահեղ լուծում է: Հաճախ, երբ խոսքը տեղեկատվության էներգիայից կախում չունեցող սարքավորումների ամբողջապես առգրավման կամ համացանցում տեղադրված ինֆորմացիայի զննության մասին է, մասնագետի մասնակցությունը ոչ միշտ է նպատակահարմար:

Վերոնշյալ խնդրի լուծումը տեսնում ենք օրենսդրորեն որոշակի խումբ հանցագործությունների քննության ընթացքում (համակարգչային անվտանգության դեմ ուղղված, համակարգչային ծրագրերի կամ սարքավորումների օգտագործմամբ իրականացվող այլ հանցագործություններ) տեղեկատվության էլեկտրոնային կրիչի առգրավմանը, էլեկտրոնային պատճենահանմանը, էլեկտրոնային կրիչի բովանդակության զննությանը մասնագետի պարտադիր մասնակցության վերաբերյալ դրույթի սահմանումը: Վերոնշյալ խումբ հանցագործությունների քննության ընթացքում միանշանակ է, որ անհրաժեշտ է կիբեռնետիկայի ոլորտի մասնագետների մասնակցությունը: Մնացած դեպքերում մասնագետի մասնակցության նպատակահարմարությունը ունի իրավիճակային բնույթ: Մասնավորապես, երբ խոսքը էներգիայից կախված սարքավորումների մասին է, առգրավման կամ դրա բովանդակության զննման մասին, կարծում ենք՝ մասնագետի մասնակցությունը անհրաժեշտ է: Էներգիայից կախում չունեցող կրիչների առգրավման ժամանակ, երբ այն սահմանափակվում է կրիչների փաթեթավորմամբ, կարծում ենք, մասնագետի մասնակցությունը պարտադիր չէ:

Ամփոփելով կարող ենք հանգել հետևյալ եզրահանգումների.

1. Թվային խուզարկությունը որպես ինքնուրույն քննչական գործողություն նախատեսելը նախևառաջ բխում է միջազգային պահանջներից, բացի այդ՝ հնարավորություն է տալիս թիրախավորել բացառապես էլեկտրոնային տվյալները՝ հաշվի առնելով վերջիններիս առանձնահատկությունները,

2. էլեկտրոնային պատճենահանման հնարավորության նախատեսումը բխում է միջազգային պարտավորություններից, բացի այդ՝ հաճախ տվյալների ձեռքբերման ամենանպատակահարմար, երբեմն միակ հնարավոր գործողությունն է, բացի այդ՝ կրկնօրինակում իրականացնելու հնարավորությունը բխում է վարույթի մասնավոր մասնակիցների շահերի ապահովման անհրաժեշտությունից,

3. էլեկտրոնային պատճենահանում իրականացնելու հնարավորությունը չի բացառում էլեկտրոնային կրիչների առգրավումը, որը մի շարք դեպքերում մնում է անփոխարինելի: Դրանք ինքնուրույն ճանաչողական միջոցներ են, որոնք որոշակի պայմանների դեպքում կարող են փոխարինել կամ հաջորդել միմյանց: Խնդիրը տարբերակված մոտեցում ցուցաբերելու հնարավորություն ապահովելն է:

4. Նոր օրենսգրքով թվային խուզարկությունը դարձել է նախնական դատական վերահսկողության առարկա: Թվային կրիչներում պահվող էլեկտրոնային տվյալների որոնման համար անհրաժեշտ է դատարանի թույլտվություն՝ հաշվի առնելով այն հանգամանքը, որ դա միջամտություն է անձի մասնավոր կյանքի անձեռնխելիության իրավունքին:

5. Քրեադատավարական օրենսդրությունը միջազգային չափանիշներին համապատասխանեցնելու համար անհրաժեշտ է նախատեսել վարույթն իրականացնող մարմնի իրավունքը՝ տարածելու որոնումը այլ համակարգչային համակարգի կամ դրա մի մասի վրա, այն դեպքում, երբ իրենք ունեն հիմքեր ենթադրելու, որ պահանջվող տեղեկատվությունը պահվում է այդտեղ:

6. Համակարգչային անվտանգության դեմ ուղղված, համակարգչային ծրագրերի կամ սարքավորումների օգտագործմամբ իրականացվող այլ հանցագործությունների դեպքում թվային խուզարկություն իրականացնելու դեպքում անհրաժեշտ է նախատեսել փորձագետի պարտադիր մասնակցություն:

ЦИФРОВОЙ ОБЫСК КАК НОВОЕ СЛЕДСТВЕННОЕ СЕЙСТВИЕ, СОГЛАСНО НОВОМУ УГОЛОВНО-ПРОЦЕССУАЛЬНОМУ КОДЕКСУ РА

Лара Петросян
Соискатель кафедры уголовного процесса и криминалистики ЕГУ,
ассистент Защитника прав человека РА

В новом Уголовно-процессуальном кодексе Республики Армения в качестве нового следственного действия был предусмотрен цифровой обыск с целью обеспечения эффективного поиска электронных данных, хранящихся в компьютерных системах. В данной статье автор обсуждает необходимость определения цифрового поиска как самостоятельного следственного действия в свете особенностей электронной информации, также рассматривает преимущества установленных правовых регулирований. В то же время автор выявил ряд недостатков на основе международных стандартов касательно обыска и выемки компьютерных данных.

DIGITAL SEARCH AS A NEW INVESTIGATIVE ACTION ACCORDING TO THE NEW CRIMINAL PROCEDURE CODE OF THE REPUBLIC OF ARMENIA

Lara Petrosyan
Applicant at the YSU Chair of Criminal Processing and Criminalistics,
Assistant to the Human Rights Defender of the RA

The new Criminal Procedure Code of the Republic of Armenia envisages digital search as a new investigative action in order to make the search of electronic data stored in computer systems effective. In the submitted article, the author discusses the necessity of defining digital search as an independent investigative action in the light of peculiarities of electronic data, as well as analyzes the benefits of envisaged legal regulations. At the same time, the author identifies a number of shortcomings based on international standards for search and seizure of computer data.

Բանալի բառեր – *համակարգչային համակարգ, էլեկտրոնային ապացույցներ, պահված համակարգչային տվյալներ, խուզարկություն, առգրավում, պատճենահանում*
Ключевые слова: *компьютерная система, электронные доказательства, хранимые компьютерные данные, обыск, выемка, копирование*
Key words: *computer system, electronic evidence, stored computer data, search, seizure, copy*